Google Scholar BETA

Web Images Video News Maps more »

+key +update +encryption +generation Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar All articles - Recent articles Results 1 - 10 of about 28,000 for +key +update +encryption -

A forward-secure public-key encryption scheme- ▶psu.edu [PDF]
R Canetti, S Halevi, J Katz - Journal of Cryptology, 2007 - Springer
... N invocations of the Boneh–Franklin identity-based encryption scheme [9 ... only; this improves the efficiency of our key-generation and key-update algorithms ...
Cited by 217 - Related articles - Web Search - BL Direct - All 33 versions

Intrusion-resilient public-key encryption- ▶jaist.ac.jp [PDF]
Y Dodis, M Franklin, J Katz, A Miyaji, M Yung - Lecture Notes in Computer Science, 2003 - Springer
... key update occurs immediately after key generation to obtain ... occurs immediately after every key update to obtain ... the case for forward-secure encryption schemes ...
Cited by 46 - Related articles - Web Search - BL Direct - All 8 versions

Protecting against key-exposure: strongly key-insulated encryption with optimal threshold- ▶psu.edu [PDF]
M Bellare, A Palacio - Applicable Algebra in Engineering, Communication and ..., 2006 - Springer
... 5]. A key-updating encryption scheme KUS ... is as follows: • The randomized key-generation algorithm KG ... the helper applies the helper key-update algorithm HKU ...
Cited by 34 - Related articles - Web Search - BL Direct - All 6 versions

A generic construction for intrusion-resilient public-key encryption- ▶psu.edu [PDF]
Y Dodis, M Franklin, J Katz, A Miyaji, M Yung - Lecture Notes in Computer Science, 2004 - Springer
... specify a key-evolving encryption scheme (with ... fsKeyGen: key generation algorithm Input: security parameter k ... public key pk fsKeyUpd: key-update algorithm Input ...
Cited by 21 - Related articles - Web Search - BL Direct - All 9 versions

Robust key-evolving public key encryption schemes- ▶psu.edu [PDF]
WG Tzeng, ZJ Tzeng - Lecture Notes in Computer Science, 2002 - Springer
... also sets TA for interacting with the decryptor to update the private ... The public key PK is treated identically to that in a standard encryption model for ...
Cited by 18 - Related articles - Web Search - BL Direct - All 8 versions

Adaptively-secure, non-interactive public-key encryption- ▶iacr.org [PDF]
R Canetti, S Halevi, J Katz - TCC, 2005 - Springer
... Enc, Dec) are the key generation, encryption, and decryption ... Adaptively-Secure, Non-interactive Public-Key Encryption ... is the secret-key update algorithm that ...
Cited by 15 - Related articles - Web Search - All 13 versions

Encryption system key distribution method and apparatus
JR Everhart, JG Osborn - US Patent 4,578,531, 1986 - Google Patents
... Firm—David H. Tannenbaum [57] ABSTRACT Encryption systems typically ... LINK KEYS EBA DBA YES UPDATE VERIFICATION INFORMATION ... A,B \ MESSAGE \ USING IATE KEY EBA ...
Cited by 46 - Related articles - Web Search - All 7 versions

A forward-secure public-key encryption scheme- ▶kfupm.edu.sa [PDF]
J Katz, R Canetti, S Halevi - papers.ssrn.com
... define a notion of security for forward-secure public- key encryption and give ... in particular, the public-key size and the key-generation/key-update times are ...

Cited by 21 - Related articles - Web Search - All 7 versions

[PDF] ▶Key distribution and management for conditional access system on DBS
W Lee - Proc. Int. Conf. Cryptology and Information Security, 1996 - dspace.lib.fcu.edu.tw
... The symmetric algorithm is used and the seed value and encryption key used in ... 3.6 Distribution and update The procedure of key distribution carried ...
Cited by 23 - Related articles - Web Search - All 3 versions

A temporal key management scheme for secure broadcasting of XML documents
E Bertino, B Carminati, E Ferrari - Proceedings of the 9th ACM conference on Computer and ..., 2002 - portal.acm.org
... based on the use of encryption techniques, and ... The proposed key assignment scheme has the additional ... the source portions which are affected by the update. ...
Cited by 36 - Related articles - Web Search - All 3 versions

Key authors: J Katz - Y Dodis - R Canetti - M Yung - S Halevi

Gooooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 Next